

1 CLAIM AMENDMENTS

2 Listing of Claims:

3 CLAIMS

4 1. (currently amended) A method for detecting attacks on a data  
5 communications network having a plurality of addresses for  
6 assignment to data processing systems in the network, the method  
7 comprising: identifying data traffic on the network originating  
8 at any assigned address and addressed to any unassigned address,  
9 said unassigned address is an address which is free and not  
10 assigned to user systems; inspecting any data traffic so  
11 identified for data indicative of an attack; and, on detection of  
12 data indicative of an attack, generating an alert signal.

13 2. (original) A method as claimed in claim 1, wherein the  
14 inspecting comprises spoofing replies to requests contained in  
15 the data traffic identified.

16 3. (original) A method as claimed in claim 1, comprising, on  
17 generation of the alert signal, rerouting any data traffic  
18 originating at the address assigned to the data processing system  
19 originating the data indicative of the attack to a disinfection  
20 address on the network.

21 4. (original) A method as claimed in claim 1, comprising, on  
22 generation of the alert signal, sending an alert message to the  
23 disinfection address.

1 5. (original) A method as claimed in claim 5, wherein the alert  
2 message comprises data indicative of the attack detected.

3 6. (original) A method as claimed in claim 5, comprising, on  
4 receipt of the alert message, sending a warning message from the  
5 disinfection address to the address assigned to the data  
6 processing system originating the data indicative of the attack.

7 7. (original) A method as claimed in claim 6, comprising  
8 including in the warning message program code for eliminating the  
9 attack when executed by the data processing system originating  
10 the data indicative of the attack.

11 8. (currently amended) Apparatus for detecting attacks on a data  
12 communications network having a plurality of addresses for  
13 assignment to data processing systems in the network, the  
14 apparatus comprising: an intrusion detection sensor for  
15 identifying data traffic on the network originating at any  
16 assigned address and addressed to any unassigned address, said  
17 unassigned address is an address which is free and not assigned  
18 to user systems inspecting any data traffic so identified for  
19 data indicative of an attack, and, on detection of data  
20 indicative of an attack, generating an alert signal.

21 9. (original) Apparatus as claimed in claim 8, wherein the  
22 intrusion detection sensor in use inspects the data traffic  
23 identified by spoofing replies to requests contained in the data  
24 traffic identified.

25 10. (original) Apparatus as claimed in claim 8, further  
26 comprising a router connected to the intrusion detection sensor  
27 for rerouting, in response to generation of the alert signal, any  
28 data traffic originating at the address assigned to the data

1 processing system originating the data indicative of the attack  
2 to a disinfection address on the network.

3 11. (original) Apparatus as claimed in claim 8, wherein the  
4 intrusion detection sensor, on generation of the alert signal,  
5 sends an alert message to the disinfection address.

6 12. (original) Apparatus as claimed in claim 11, wherein the  
7 alert message comprises data indicative of the attack detected.

8 13. (original) Apparatus as claimed in claim 12, further  
9 comprising a disinfection server assigned to the disinfection  
10 address, the disinfection server sending, on receipt of the alert  
11 message, a warning message to the address assigned to the data  
12 processing system originating the data indicative of the attack.

13 14. (original) Apparatus as claimed in claim 13, wherein the  
14 warning message comprises program code for eliminating the attack  
15 when executed by the data processing system originating the data  
16 indicative of the attack.

17 15. (currently amended) A data communications network comprising:  
18 a plurality of addresses for assignment to data processing  
19 systems in the network; and, apparatus for detecting attacks on  
20 the network as claimed in claim 8 ~~any of claims 8 to 14~~.

21 16. (currently amended) A computer program element comprising  
22 computer program code means which, when loaded in a processor of  
23 a data processing system, configures the processor to perform a  
24 method for detecting attacks on a data communications network as  
25 claimed in claim 1 ~~any of claims 1 to 7~~.

1 17. (original) A method as claimed in claim 1, further comprising  
2 supporting an entity in the handling of the detected attack by  
3 one of providing instructions for use of, assistance in  
4 executing, and execution of disinfection program code.

5 18. (original) A method as claimed in claim 1, further comprising  
6 providing a report to said entity containing information related  
7 to one of alert, disinfection, rerouting, logging, discarding of  
8 data traffic in the context of a detected attack.

9 19. (original) A method as claimed in claim 1, further comprising  
10 billing said entity for the execution of at least one of the  
11 steps contained in claim 1 ~~claims 1 to 7~~, the charge being billed  
12 preferably being determined in dependence of one of the size of  
13 the network, the number of unassigned addresses monitored, the  
14 number of assigned addresses monitored, the volume of data  
15 traffic inspected, the number of attacks identified, the number  
16 of alerts generated, the signature of the identified attack, the  
17 volume of rerouted data traffic, the degree of network security  
18 achieved, the turnover of said entity.

19 20. (original) A method as claimed in claim 1, further comprising  
20 providing said method for several entities and using technical  
21 data derived from the attack-handling for one of said entities  
22 for the attack-handling for another of said entities.

23 21. (currently amended) A method for deploying an intrusion  
24 detection application for an entity, comprising:  
25 connecting an intrusion detection sensor to a network used by  
26 said entity for identifying data traffic on the network  
27 originating at any assigned address and addressed to any  
28 unassigned address, said unassigned address is an address which  
29 is free and not assigned to user systems, and for inspecting any

1 data traffic so identified for data indicative of an attack and  
2 for, on detection of data indicative of an attack, generating an  
3 alert signal,  
4 - connecting a router to said network for rerouting, in  
5 response to generation of the alert signal, any data traffic  
6 originating at the address assigned to the data processing system  
7 originating the data indicative of the attack to a disinfection  
8 address on the network.

9 22. (original) A method according to claim 21, further comprising

10  
11 - connecting a disinfection server assigned to the  
12 disinfection address, to the network, the disinfection server  
13 being adapted for sending, on receipt of the alert message, a  
14 warning message to the address assigned to the data processing  
15 system originating the data indicative of the attack.

16 23. (new) A computer program product comprising a computer  
17 usable medium having computer readable program code means  
18 embodied therein for causing detection of attacks on a data  
19 communications network having a plurality of addresses for  
20 assignment to data processing systems in the network, the  
21 computer readable program code means in said computer program  
22 product comprising computer readable program code means for  
23 causing a computer to effect the functions of claim 1.

24 24. (new) A computer program product comprising a computer usable  
25 medium having computer readable program code means embodied  
26 therein for causing deployment of an intrusion detection  
27 application for an entity, the computer readable program code  
28 means in said computer program product comprising computer  
29 readable program code means for causing a computer to effect the  
30 functions of claim 21.